REMARKS

Claims 1, 3, 7-11, 13, 14, 17 and 19 are amended. Claims 6, 18, and 20 are cancelled. Claims 1-5, 7-17, and 19 remain in the application.

The amendments to claim 1 incorporate limitations from cancelled claim 6 and also set forth the ability of the scrambling circuit to selectively scramble data frames by either encrypting only frame information, or encrypting frame information and selectively encrypting frame overhead. Claim 13 has been amended to set forth the selective scrambling alternatives. These amendments are supported in the specification at page 12, lines 9-23 of the specification. The amendments to claim 19 incorporate the limitations of cancelled claim 20. The remaining amendments either rationalize dependency or rectify informalities. None of these amendments introduces new matter.

Claims 1-7, 9, 10, 13-16, and 18-20 are rejected for anticipation by US Patent 5881154 ("Nohara"). This rejection is moot with respect to claims 6, 18, and 20, which have been cancelled, and is respectfully traversed for the following reasons.

Claims 1-5, 7, 9, and 10

Claim 1 recites an encryption system including a frame generator that frames information and divides "each frame into time multiplexed sections including a first frame period including information, and a second frame period including overhead," and generates an "output to provide timing information regarding the occurrence of the first and second frame periods." A scrambling circuit responds to the timing information by "selectively scrambling each frame" by either:

"encrypting only the information section of the frame; or

encrypting the information section of the frame, and selectively encrypting the overhead section of the frame."

The Nohara data scramble transmission system scrambles only the data portion of a detected transmission frame. See Nohara's Abstract and also Nohara's description at column 4, lines 54-59. After scrambling the data portion

of a frame, the frame is reconstituted and sent. See Nohara at column 4, lines 60-65. At column 1, lines 25-45, Nohara also describes a prior art frame synchronization scramble device that scrambles an entire frame based upon a single predetermined polynomial. However, Nohara does not describe or teach "selectively" scrambling a frame by encrypting either "only" the data or encrypting the data and "selectively encrypting the overhead" of a frame. In fact Nohara teaches away from encrypting any part of a frame's overhead. See column 1, lines 46-53. Accordingly, Nohara does not anticipate these claims.

Claims 13-16

Claim 13 concerns a method for encrypting transmissions in which information to be transmitted is accepted and organized into frames "including time multiplexed sections of information and sections of overhead". The method includes:

"self-synchronously scrambling the frames by either encrypting only the information sections in accordance with a first predetermined encryption pattern or by encrypting the information sections in accordance with the first predetermined encryption pattern and selectively encrypting the overhead sections in accordance with a second predetermined encryption pattern", and then transmitting the scrambled frames.

As set forth above, Nohara does not describe or teach "scrambling" a frame by encrypting either "only" the data or encrypting the data and "selectively encrypting the overhead" of a frame. As stated, Nohara teaches away from encrypting any part of a frame's overhead. See column 1, lines 46-53. Accordingly, Nohara does not anticipate these claims.

Claim 19

As amended, claim 19 corresponds essentially with cancelled claim 20. In this regard, a sabotage prevention system includes "a means for self-synchronously and continuously scrambling" frames from an assembly means, subsequent to assembly of the frames, "in which said self-synchronous scrambling means includes control inputs with timing data that are synchronous to at least one overhead bit in the frame to disable said scrambling means, whereby the scrambling operation becomes modifiable."

The contention in the Office Action at page 7, last paragraph is that the claimed subject matter is taught in Nohara at column 1, lines 32-44. The applicant respectfully disagrees. What Nohara describes is a prior art scramble device with a scramble pattern generator 13 that produces a random signal pattern in response to the order of control frames from a data interface. The randomness of the signal pattern is based upon "a predetermined polynomial and upon an initial data pattern". But there is no description of "at least one overhead bit in the frame to disable" the scramble pattern device or the scramble pattern generator 13. Accordingly, Nohara does not anticipate claim 19.

Claims 8, 11, and 17 are rejected over Nohara in view of US Patent 5442703 ("Kim") in view of US Patent 5303303 ("White"). This rejection is respectfully traversed for the following reasons.

As conceded in the Office Action at page 8, second paragraph, "Nohara does not teach encrypting the overhead bits with a second predetermined encrypted pattern." In fact, Nohara disfavors the encryption of overhead bits at all in view of the increase in transmission rate that accompanies the encryption of an entire frame. See Nohara at column 1, lines 46-53. Indeed, one of Nohara's objects is to scramble frame data "whereby it is not necessary to change the data rate and the transmission format." Nohara at column 2, lines 35-38. In order to accomplish this objective, framing bits are temporarily stored while data bits are scrambled by de-interleaving, and then the framing bits are added to the de-interleaved data "to reconstitute the frame." See Nohara at column 3, lines 55-65. Accordingly, Nohara teaches away from including "overhead bits" in frame

scrambling operations. Therefore, there is no suggestion or motivation to combine Nohara with any reference teaching encryption of frame overhead bits.

The contention in the Office Action at page 8, second paragraph is that White teaches separate encryption of overhead and data at column 1, lines 43-45. The applicant respectfully disagrees. White in fact teaches encryption of a first packet containing an entire frame, and then generating a second packet by appending further header and trailer portions on the encrypted frame. The passage does not teach that the header and trailer portions of the first packet are encrypted separately from the information portion, nor does it teach that the second packet is encrypted. Kim teaches the use of multiple encryption keys for communications systems, however multiple keys are kept in order that a failed key be replaced with a default key. Kim does teach that key failure is the criteria for use of different encryption keys, but does not teach that encryption keys are changed in response to different forms of data. Therefore, even if White and Kim were combined with Nohara, the combination omits encrypting "the information section of the frame in accordance with a first predetermined encryption pattern," and selectively encrypting "the overhead section of the frame in accordance with a second predetermined encryption pattern." Accordingly, these claims are not obvious over Nohara in view of White and Kim.

Therefore, all claims remaining in the application are patentably distinguishable from the references of record.

Respectfully submitted,

Terrance A. Meador

Date: April 2, 2004

TERRANCE A. MEADOR
Reg. No. 30, 298

INCAPLAW
1050 Rosecrans Street, Suite K
San Diego, CA. 92106

619-222-2531 (Office) 619-222-2327 (FAX)